Eschatology, Infinite Series, and Reliability

Becker, Peter W.

Published in:
I E E E Transactions on Reliability

Link to article, DOI:
10.1109/TR.1982.5221274

Publication date:
1982

Document Version
Publisher's PDF, also known as Version of record

Eschatology, Infinite Series, and Reliability

Peter W. Becker, Member IEEE
Technical University of Denmark, Lyngby

Key Words—**Infinite series, Eschatology, ICBM attack, False alarms, Retaliatory action.**

Reader Aids—
Purpose: To describe a simple model for estimating system reliability
Special math needed for explanations: Infinite products and sums
Special math needed for results: Evaluation of infinite products and sums
Results useful to: System analysts

Abstract—**This communication is concerned with a most timely problem. Early warning systems against ICBM-attacks now and then cause false alarms which in turn can trigger a retaliatory ICBM attack. Up until now any retaliatory attacks have been stopped before any consequences have resulted. I try to compute the joint probability of infinitely many false alarms being detected before serious consequences have resulted.**

1. INTRODUCTION

In the field of theology the body of doctrines concerned with the last and final things such as death & resurrection are collectively referred to as eschatology. Doctrines about "an all out ICBM attack having been launched a few minutes ago, and immediately to be countered by a retaliatory ICBM attack" ought to be added to this older and more venerable body of doctrines.

With this communication I propose a somewhat naïve way of computing the joint probability of all false alarms in the early warning systems being detected before they cause a holocaust.

The definition of reliability depends very much on the nature of the subject matter; e.g. the reliability of a safety match, a transistor, or an early warning system must be defined using different concepts. How the reliability of an early warning system should be defined I leave open for discussion; somehow the consequences of system errors—be they small or of worldwide importance—should be reflected in the definition.

2. MODEL FOR FALSE ALARMS

By now it has become regular fare on our newsmedia to learn that the Pentagon for so and so many minutes believed that a full scale ICBM attack on the USA had just been launched and retaliation has been initialized. Considering that the Wimex-System and the other parts of the US early warning system probably are no worse than their counterparts in the USSR, UK, and France, such news should be regarded as testimony to American frankness rather than to shoddy engineering.

In this communication I am specifically concerned with the question: what is the joint probability of each and every false alarm being recognized as such in time, i.e. before it has apocalyptic consequences? To answer the question one has to develop a mathematical model for the false alarms. Like all other big systems, early warning systems against an ICBM-attack have potential for malfunctioning and what we are experiencing is simply a debugging of systems at the peril of survival of mankind. The following assumes that all false alarms are taken seriously and believed in by the staff.

Let us define some concepts and make some assumptions. One cause for false alarm might be that a flight of wild geese under certain circumstances causes radar reflections similar to those of oncoming enemy ICBMs. This may be false alarm Type 1. We assume that with constant probability p_1 the alarm is recognized as being false before retaliatory action is taken, and that the Type 1 false alarm will cause retaliatory action with probability $(1-p_1)$. False alarm Type 2 could be one caused by human error; e.g. a tape with radar return data simulating an enemy attack is read while the staff believes that the data are live radar return data. We assume that with constant probability p_2 the alarm is recognized as being false before retaliatory action is taken; and that the Type 2 false alarm will cause retaliatory action with probability $(1-p_2)$. We assume that the total number of false alarm types is m and that with constant probability p_i, $i = 1, 2, \ldots, m$, false alarm Type i is recognized as being false before retaliatory action is taken.

Next let us list the assumptions on which the model is based.

1. If Type i false alarm is not recognized as such in time, and that happens with constant probability $(1-p_i)$, this constitutes the end in so far as our model is concerned; there will be no further debugging.
2. When false alarm Type i is recognized as such in time its causes are completely removed from the system, i.e. a Type i false alarm will not occur twice.
3. The probability, p_i, of recognizing false alarm Type i as such is independent of what false alarms up until then have been recognized as such in time and have had their underlying courses remedied; i.e. the outcomes of checking false alarms are statistically independent. Whereas Assumptions 1 and 2 should be readily acceptable, the validity of Assumption 3 needs to be verified for each particular system.

If we are fortunate enough to recognize all false alarms as such and we wait long enough all, then m types will have appeared (in some arbitrary order) and the system will have been completely debugged with probability P_m.

$$P_m = p_1 \cdot p_2 \cdots p_i \cdots p_m,\ 0 < p_i < 1$$

0018-9529/82/0600-0135$00.75

3. VALUES OF INFINITE PRODUCTS

Should the reader be interested in just a rough (and pessimistic) estimate of P_m, one simple procedure is to consider the case where m goes to infinity and then consult the literature on infinite products [1] to see if there is one where the factors fit his model. The value of P_∞ may be zero or take a non-zero value; e.g. Wallis' product can be written as:

$$\pi/4 = (8/9) \cdot (24/25) \cdot (48/49) \cdot (80/81) \cdot (120/121) \cdots\cdots$$

Also infinite sums [1] are of interest because "$S_\infty = s_1 + s_2 + \cdots$" can be transformed to an infinite product $\exp S_\infty = (\exp s_1) \cdot (\exp s_2) \cdots$.

The value $P_\infty = 0$ indicates that disaster is certain if only one waits long enough. However, for some infinite products P_∞ takes a non-zero value. Ways of bounding the value of P_∞ have been described in the literature [2]. One procedure is to compare the factors in the P_∞, one by one, with the factors in some infinite product the value of which is known. The following example illustrates the procedure. Assume that there exist two numbers L and H for which it holds true that:

$$L \leqslant (\log p_{i+1})/(\log p_i) \leqslant H, \qquad i = 1, 2, \cdots$$

then (and recalling that $\log p_i$ is a negative number):

$$-\log P_\infty \leqslant -(\log p_1)(1 + H + H^2 + \cdots)$$
$$= -(\log p_1)/(1 - H)$$

$$-\log P_\infty \geqslant -(\log p_1)(1 + L + L^2 + \cdots)$$
$$= -(\log p_1)/(1 - L)$$

$$p_1^{1/(1-L)} \geqslant P_\infty \geqslant p_1^{1/(1-H)}.$$

4. CONCLUSIONS

The theoretical aspects of catastrophe theory; a branch of applied mathematics invented by René Thom about ten years ago, have been discussed elsewhere [3] and are still being studied at special conferences. In this communication I have addressed a problem much more limited in scope, a problem which is of interest not only to disaster-buffs and latter-day-eschatologists but of grave concern to us all: what is the probability that an error in an early warning system might trigger an uncalled-for retaliatory attack?

5. ACKNOWLEDGMENTS

I thank Mr. Hugh Tucker and Mr. H. Elbrønd Jensen for valuable help.

REFERENCES

[1] K. Knopp, "Infinite sequences and series", N.Y.: Dover Publications, 1956.

[2] T.M. Apostol, "Mathematical analysis", Reading, Mass.: Addison-Wesley, 1957.

[3] E.C. Zeeman, "Catastrophe theory", *Scientific American,* 1976 Apr, pp 65-83.

AUTHOR

Dr. Peter W. Becker; Electronics Laboratory, Bldg. 344; Technical University of Denmark; DK-2800 Lyngby, DENMARK.

Dr. Peter W. Becker: For biography, see paper by same author in this issue.

Manuscript TR80-90 received 1980 July 28; revised 1981 September 5.

★★★

From The Editors

Correspondence Items

Do you want to sound off on a reliability topic?

Then DO IT!

Write a "Letter to the Editor".

The Editorial Board welcomes your comments on material published in this Transactions (e.g., technical papers, editorials, and book reviews) as well as on topics of interest to Transactions readers. If the correspondence concerns technical matters it will be sent to the original authors and/or other capable people for their comments. The correspondent need not make any changes because of those "referee" comments, but is permitted to do so. Correspondence items are labeled as "not formally refereed" because the comments are not binding on the correspondent.

Comments on technical errors, with a reply by the original author, will usually be published as a short note. Interaction between the correspondent and the original author is encouraged in order to reduce the area of disagreement as much as feasible.

Material which is judged not suitable as a refereed paper can sometimes be abbreviated and published as a correspondence item.

Correspondence will be edited as to length and some rather broad limits of propriety — at the sole discretion of the Editor. ★★★